

Applicant: Ding, et al.  
Filed: May 15, 2006  
Amendment and Response to Non-final Office Action

## **REMARKS**

As a preliminary matter, Applicants wish to thank the Examiner for the thorough examination of the present application as evidenced in the non-final Office Action mailed July 26, 2007. The present Amendment and Response is responsive to the non-final Office Action mailed July 26, 2007. Claims 1-4, 8-16 remain pending with Claims 1, 2, 4, 11, and 13-16 being amended, and Claims 5-7 being canceled. Claims 1, 2, 4, 11, and 13-16 have been amended as described below in the sections entitled "Objections to the Claims" and the "Claim Rejections under 35 U.S.C. § 112." Reconsideration and allowance of the application, as amended, is requested.

### **Objections to the Specification**

The Office Action objected to the abstract because it exceeded 150 words in length. By the present amendment to Abstract, Applicants respectfully submit that this objection is now moot.

The Office Action also objected to some abbreviations as not being spelled out the first they are used. As shown by the present amendment, the specification has been amended to replace "SSS(x)" with "supper summit set SSS(x)" and "BCDA" with "conjugacy decision algorithm in braid groups BCDA." Accordingly, Applicants respectfully request this objection be withdrawn.

### **Objections to the Claims**

The Office Action requested that the range of "20~30" in Claims 4, 11, and 13-16 be changed to "20~28" based upon Table II of the specification. While Applicants believe the specification supports at least the range of "20~30", Applicants have amended the range in Claims 4, 11, and 13-16 to be "20~28" in accordance with the Office Action's request in order to expedite consideration and allowance of the present application.

Applicant: Ding, et al.  
Filed: May 15, 2006  
Amendment and Response to Non-final Office Action

### **Claim Rejections under 35 U.S.C. § 112**

The Office Action rejected claims 1-2 under 35 U.S.C. § 112, second paragraph, as being indefinite based upon insufficient antecedent basis for certain features of the claims. Applicants respectfully submit that Claims 1 and 2 have been amended to provide sufficient antecedent basis for all claim features, and accordingly request that the claim rejections under 35 U.S.C. § 112 be withdrawn.

### **Claim Rejections Under 35 U.S.C. § 102**

The Office Action rejected Claims 1-4 and 13-14 under 35 U.S.C. § 102(b) as being anticipated by K.H. Ko et al., “New signature Scheme Using Conjugacy Problem,” November 11, 2002, pages 1-13 (hereinafter referred to as the “cited reference” for convenience).

Independent Claim 1 provides for digital signature schemes based on braid group conjugacy. Compared with the digital signature method provided by the cited reference cited in the Office Action, a distinguishing feature of Claim 1 is as follows: in the digital signature scheme provided by Claim 1, the braid group  $B_n(l)$  is divided into a left subgroup  $LB_m(l)$  and a right subgroup  $RB_{n-l-m}(l)$ , and in Step 3, a random braid  $b$  is generated in the right subgroup  $RB_{n-l-m}(l)$  of the braid group based on the exchangeability of the left and right subgroups (see the related description in the specification, page 2, paragraph [0049] of Publication No. 2007/0104322A1); while the digital signature method disclosed in the cited reference (section 2.3 on page 4-5) does not involve the concepts that the braid group is divided into a left subgroup and a right subgroup, and the random braid  $b$  is generated within the whole braid group. Therefore, independent Claim 1 is allowable over the cited reference.

Moreover, the digital signature scheme recited in independent Claim 1 provides for several non-obvious advantages over the digital signature method of the cited reference. Compared with the digital signature method disclosed in the cited reference, the digital signature scheme of Claim 1, in which the braid group is divided into a left subgroup and a right subgroup, and a random braid is generated in one subgroup of the braid group based on the exchangeability of the left and right subgroups, decreases the number of braids used and the times of conjugacy

determination without reducing the security, avoids the excessive consumption of calculation resource, the overlong time for generating private key and verifying signature, and the overlong signature data, thereby improves the calculating efficiency of signature greatly and reduces the length of signature (see the related description in the specification, page 2, paragraph [0049] to page 3, paragraph [0051] of Publication No. 2007/0104322A1). Accordingly, based upon these non-obvious advantages, Applicants respectfully submit that independent Claim 1 is not obvious in view of the cited reference. Likewise, Applicants respectfully submit that there is no teaching or suggestion to modify the cited reference to obtain all of the features recited in independent Claim 1. Accordingly, independent Claim 1 remains patentable over the cited reference.

Dependent Claims 2-4 and 13-16, which depend from independent Claim 1, are allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features.

#### **Claim Rejections Under 35 U.S.C. § 103**

The Office Action rejected Claims 8-12 and 15-16 under 35 U.S.C. § 102(b) as anticipated by or, in the alternative, under 35 U.S.C. § 103(b) as obvious over K.H. Ko et al., "New signature Scheme Using Conjugacy Problem," November 11, 2002, pages 1-13 (hereinafter referred to as the "cited reference" for convenience).

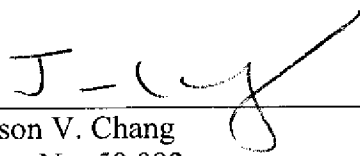
Applicants respectfully submit that independent Claim 8, which recites similar patentable features as independent Claim 1, is allowable for at least similar reasons discussed above with respect to independent Claim 1. Dependent Claims 9-12 and 15-16, which dependent from independent Claim 8, are allowable as a matter of law as depending from an allowable base claim, notwithstanding their independent recitation of patentable features.

Applicant: Ding, et al.  
Filed: May 15, 2006  
Amendment and Response to Non-final Office Action

**CONCLUSION**

The Applicants believe they have responded to each matter raised by the Examiner. Allowance of the claims is respectfully solicited. It is not believed that extensions of time or fees for addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 19-5029.

Respectfully submitted,

  
\_\_\_\_\_  
Jason V. Chang  
Reg. No. 58,092

**DATE: October 23, 2007**

SUTHERLAND ASBILL & BRENNAN LLP  
999 Peachtree Street, NE  
Atlanta, Georgia 30309-3996  
Telephone: (404) 853-8214  
Facsimile: (404) 853-8806  
SAB Docket No.:25515-0002